

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
Takuya KOBAYASHI et al. :
Serial No. NEW : **Attn: APPLICATION BRANCH**
Filed January 17, 2002 : Attorney Docket No. 2002_0037A
DATA PROCESSOR

CLAIM OF PRIORITY UNDER 35 USC 119

Assistant Commissioner for Patents,
Washington, DC 20231

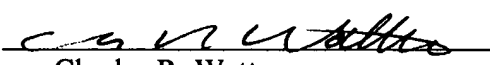
Sir:

Applicants in the above-entitled application hereby claim the dates of priority under the International Convention of Japanese Patent Application No. 2001-011247, filed January 19, 2001, Japanese Patent Application No. 2001-011254, filed January 19, 2001, and Japanese Patent Application No. 2001-011248, filed January 19, 2001, as acknowledged in the Declaration of this application.

Certified copies of said Japanese Patent Applications are submitted herewith.

Respectfully submitted,

Takuya KOBAYASHI et al.

By 
Charles R. Watts
Registration No. 33,142
Attorney for Applicants

CRW/asd
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
January 17, 2002

日 本 国 特 許 庁
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2001年 1月19日

出 願 番 号
Application Number:

特願2001-011247

出 願 人
Applicant(s):

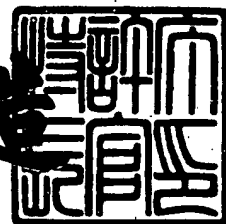
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年11月30日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3105304

【書類名】 特許願

【整理番号】 2037320013

【提出日】 平成13年 1月19日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/32

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 小林 卓也

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 稲見 聡

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 水山 正重

【発明者】

【住所又は居所】 神奈川県横浜市港北区綱島東四丁目3番1号 松下通信工業株式会社内

【氏名】 加藤 淳展

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 データ処理装置

【特許請求の範囲】

【請求項 1】 受信したデータを処理するデータ処理装置であって、前記データは、

改竄を検出するための情報を納める検証情報領域と、改竄検出対象とするデータを納める保護データ領域と、改竄検出対象外のデータを納める非保護データ領域から構成され、さらに前記非保護データ領域に納めるデータの種別を前記保護データ領域内に非保護対象リストとして保持することを特徴とし、

前記データ処理装置は、前記保護データ領域内のデータ改竄を検出する署名検証手段と、前記非保護データ領域内のデータについて前記非保護対象リストで定義されたデータかどうかを検証する非保護データ検証手段とを備えることを特徴とするデータ処理装置。

【請求項 2】 受信するデータをハイパーテキストとし、前記非保護対象リストには前記非保護データ領域に使用するタグのリストを保持する請求項 1 記載のデータ処理装置。

【請求項 3】 互いに通信によってデータを交換しあう複数のデータ処理装置であって、前記データは、改竄を検出するための情報を納める検証情報領域と、改竄検出対象とするデータを納める保護データ領域と、改竄検出対象外のデータを納める非保護データ領域から構成され、さらに前記非保護データ領域に納めるデータの種別を前記保護データ領域内に非保護対象リストとして保持することを特徴とし、

送信側データ処理装置は、前記保護データ領域のデータについて改竄の有無を検出するための前記検証情報領域を作成する署名生成部と、前記非保護データ領域で使用する情報のリストを前記非保護対象リストに定義する非保護対象リスト生成部とを備え、

受信側データ処理装置は、前記保護データ領域内のデータ改竄を検出する署名検証手段と、前記非保護データ領域内のデータについて前記非保護対象リストで定義されたデータかどうかを検証する非保護データ検証手段とを備えることを特

徴とするデータ処理装置。

【請求項4】 通信に用いるデータをハイパーテキストとし、前記非保護対象リストには前記非保護データ領域に使用するタグのリストを保持する請求項3記載のデータ処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークに接続してコンテンツを送受信する通信システムに属し、より特定のにはデータの改竄を検出し信頼性の高い通信を行う情報処理端末に属する。

【0002】

【従来の技術】

近年、インターネットに接続されるコンピュータの著しい増大により、特にWWW（ワールドワイドウェブ、以下ウェブと示す）閲覧が盛んになっている。ウェブ閲覧においてはコンテンツのダウンロードや表示だけでなく、オンラインでのショッピング、トレードなどにも利用されるようになってきている。

【0003】

これらの目的でデータをやりとりする場合は、送受信するデータに高い信頼性が要求される。すなわち正しい相手から送信されたデータであるか確認し、第三者によるハッキングなどデータの改竄が行われていないか正しく検出し、誤ったデータで処理を行わないようにしなければならない。通信データについて高い信頼性を保証する方法として、公開鍵暗号を用いたデジタル署名の方法が知られている。以下、その方法について述べる。

【0004】

送信側では、送信する内容（以下本文と示す）を一方向関数でハッシュ化した上、外部に公開しない秘密鍵で暗号化する。そして秘密鍵で暗号化した文字列（以下署名と示す）および秘密鍵と対になる公開鍵を本文に添付して相手に送信する。

【0005】

受信側では、受信した本文を一方向関数でハッシュ化する。また本文に添付された署名を同じく本文に添付された公開鍵で復号化する。その結果得られた文字列と、先ほど本文をハッシュ化した結果を比較する。比較結果が一致した場合、本文は秘密鍵を持っているものから送られ、かつ通信の途中で改竄が行われていないことが保証される。

【0006】

このデジタル署名方式では、署名を添付する場合も署名の検証を行う場合も本文の全てを一方向関数でハッシュ化する必要がある。したがってデータが大きくなればなるほど処理時間も処理負荷も高くなり、特に比較的処理能力の小さい携帯端末にとっては処理量の増大が問題となっていた。

【0007】

そこで全てのデータをハッシュ化するのではなく、改竄を防ぎたい重要な部分のみデジタル署名の計算対象とする方法が考えられる。例えば本文について署名を生成するためにハッシュ化の対象とする部分（以下、これを改竄から保護するという意味で保護データ領域と示す）とそうでない部分（以下非保護データ領域と示す）に分けてデータを配置し、保護データ領域のみについて署名の作成、および検証を行う。保護データ領域に書かれた内容はデジタル署名による改竄の有無のチェックが行われる。非保護データ領域についてはデジタル署名の検査対象とはしない。これにより本文のデジタル署名に要する処理負荷を最小限に押さえることが可能となる。

【0008】

【発明が解決しようとする課題】

しかしながら、上述のように本文を保護データ領域と非保護データ領域に分ける方法では、受信した側がデータ処理する場合にその情報が保護データ領域に書かれていたものか非保護データ領域に書かれていたものか常に意識して処理しなければならない。その理由は、本来保護データ領域に書かれるべき情報が非保護データ領域に書かれていたとすると、受信側は保護データ領域に書かれていた場合と同様に扱ってはならないからである。

【0009】

したがって受信側でデータを処理するアプリケーションが常に受信データについてどの情報が保護データ領域または非保護データ領域にあったかを意識して処理しなければならない。このことはデータ量が増えた場合にアプリケーションにとって大きな負担となる。

【0010】

そのためにあらかじめ送信側と受信側で保護データ領域、非保護データ領域それぞれに書くべき情報をあらかじめ合意して定めておくことが考えられる。しかしこの場合も、データの重要性が変わり、例えば非保護データ領域にある情報を改竄から防ぐため保護データ領域に記述したくなった場合に、受信側のアプリケーションを変更する必要性が生じる。このように情報の追加や保護非保護の変更が柔軟に行えないという欠点があった。

【0011】

そこで、本発明はかかる問題に鑑みてなされたものであり、保護データ領域と非保護データ領域のいずれに情報が書かれているかをアプリケーションは意識することなく、かつ重要なデータについて改竄のない高い信頼性を持った通信を実現し、非保護データ領域に置いたデータについても改竄に対して強く、さらにデジタル署名処理を効果的に行うための技術を提供する。

【0012】

さらに本発明では、アプリケーションの変更なく、データを保護データ領域に置くか非保護データ領域に置くか決定でき、データの保護レベルについて柔軟な変更が可能な技術を提供する。

【0013】

【課題を解決するための手段】

上記目的を達成するために本発明にかかるデータ処理装置は、受信したデータを処理するデータ処理装置であって、前記データは、改竄を検出するための情報を納める検証情報領域と、改竄検出対象とするデータを納める保護データ領域と、改竄検出対象外のデータを納める非保護データ領域から構成され、さらに前記非保護データ領域に納めるデータの種別を前記保護データ領域内に非保護対象リストとして保持することを特徴とし、前記データ処理装置は、前記保護データ領

域内のデータ改竄を検出する署名検証手段と、前記非保護データ領域内のデータについて前記非保護対象リストで定義されたデータかどうかを検証する非保護データ検証手段とを備えることを特徴とするデータ処理装置である。

【 0 0 1 4 】

上記構成により、本発明にかかるデータ処理装置は、保護データ領域と非保護データ領域のいずれに情報が書かれているかアプリケーションが意識することなく、かつ重要なデータの改竄を防いだ信頼性の高い通信を実現し、非保護データ領域に置いたデータについても改竄に対して強く、さらにデジタル署名処理を効果的に行うことが可能となる。

【 0 0 1 5 】

また上記目的を達成するために本発明にかかるデータ処理装置は、互いに通信によってデータを交換しあう複数のデータ処理装置であって、前記データは、改竄を検出するための情報を納める検証情報領域と、改竄検出対象とするデータを納める保護データ領域と、改竄検出対象外のデータを納める非保護データ領域から構成され、さらに前記非保護データ領域に納めるデータの種別を前記保護データ領域内に非保護対象リストとして保持することを特徴とし、送信側データ処理装置は、前記保護データ領域のデータについて改竄の有無を検出するための前記検証情報領域を作成する署名生成部と、前記非保護データ領域で使用する情報のリストを前記非保護対象リストに定義する非保護対象リスト生成部とを備え、受信側データ処理装置は、前記保護データ領域内のデータ改竄を検出する署名検証手段と、前記非保護データ領域内のデータについて前記非保護対象リストで定義されたデータかどうかを検証する非保護データ検証手段とを備えることを特徴とするデータ処理装置である。

【 0 0 1 6 】

上記構成により、本発明にかかるデータ処理装置は、アプリケーションの変更なく、データを保護データ領域に置くか非保護データ領域に置くか決定でき、データの保護レベルについて柔軟な変更が可能となる。

【 0 0 1 7 】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて詳細に説明する。

【0018】

(実施の形態1)

図1は本発明の実施の形態1におけるデータ処理装置の構成を示すシステムブロック図である。図1に示すデータ処理装置10は、外部からデータを受信する受信部101、受信したデータについてデジタル署名の検証を行う署名検証部102、デジタル署名の対象外となっている非保護データ領域のデータについて正当性をチェックする非保護データ検証部103、実際にデータを利用するアプリケーション部104からなる。

【0019】

また図2は本発明の実施の形態1におけるデータ処理装置が扱うデータの構成図である。図2に示すデータ20は、デジタル署名の対象となる保護データ領域201、デジタル署名の対象外となる非保護データ領域202、デジタル署名のための署名および公開鍵を納める検証情報領域203からなり、さらに保護データ領域201は非保護データ領域202に含む情報の種別を格納した非保護対象リスト204を保持する。

【0020】

以下図1と図2を用いて実施の形態1におけるデータ処理装置の動作について説明する。データ処理装置10は受信部101にデータを受信する。データの受信は特に図に示していないが例えばネットワークに有線または無線で接続され装置外部からデータを取得できるものとする。受信部101は受信したデータ20を署名検証部102に渡す。

【0021】

署名検証部102ではデータ20から保護データ領域201について検証情報領域203の検証情報をもとに保護データ領域201のデータに改竄や誤りが生じていないかチェックを行う。具体的には検証情報領域203は保護データ領域201をハッシュ化し送信元で秘密鍵により暗号化した署名と、秘密鍵と対をなす公開鍵からなり、署名を公開鍵で復号化して、保護データ領域201をハッシュ化した結果と比較する。保護データ領域201のデータが正しければ、比較結

果は一致するので署名検証部 1 0 2 は保護データ領域 2 0 1 と非保護データ領域 2 0 2 に含まれるデータを非保護データ検証部 1 0 3 へ渡す。

【 0 0 2 2 】

非保護データ検証部 1 0 3 では、非保護データ領域 2 0 2 のデータが保護データ領域 2 0 1 の非保護対象リスト 2 0 4 に記載された情報であるかどうかチェックを行う。非保護対象リスト 2 0 4 自体は先ほどの署名検証部 1 0 2 により正しいことが確認済みであるから、非保護対象リスト 2 0 4 にない種別のデータが非保護データ領域 2 0 2 にある場合は、改竄や誤りが発生して種別が変わってしまったか、もしくはアプリケーション 1 0 4 にとって意味のないデータである。したがって非保護データ検証部 1 0 3 は、非保護対象リスト 2 0 4 に記載された種別の情報のみを非保護データ領域 2 0 2 から選択し、保護データ領域 2 0 1 の情報と共にアプリケーション 1 0 4 に渡す。

【 0 0 2 3 】

以上の構成のように、非保護データ領域で使用する情報種別を保護データ領域内の非保護対象リストに定義することによって、データ全体に対してデジタル署名する場合に比べて署名確認に用いるデータの量が少なくなり署名検証の効率が向上する。また非保護データ領域内のデータは、改竄のない保護領域にある非保護対象リスト 2 0 4 に定義されているもののみを扱うため、データの信頼性を高く保つことが可能となる。またアプリケーションにとっては各データ毎に保護領域にある情報か非保護領域にある情報かといったことを意識しないで処理することが可能となる。

【 0 0 2 4 】

(実施の形態 2)

図 3 のテキストデータ 3 0 は公開鍵暗号によるデジタル署名を埋め込んだハイパーテキスト型言語、例えば XML (eXtensible Markup Language) で記述されたスケジュールデータである。図 3 および必要に応じて図 1 と図 2 を援用しながら本発明の実施の形態 2 について説明する。

【 0 0 2 5 】

例えばネットワークサーバ上のスケジュールと携帯端末内のスケジュール帳の

スケジュールデータがそれぞれ随時更新されている場合、データの同期を取ってスケジュールを統一する作業が必要になる。そこでクライアントからサーバに対して同期を要求すると、スケジュールの更新方法としてサーバ側優先かクライアント側優先で書き換えを行うかといった書き換え操作のコマンドや、実際のスケジュールデータや、更新日時情報や、書き換えセッションのIDがサーバからクライアントに送られるシステムを考える。

【0026】

図3のスケジュールの同期用にサーバから配送されてくるテキストデータ30において、「PROTECTED」というタグで囲まれた保護データ領域301が図2の保護データ領域201に相当する。同様に「UNPROTECTED」というタグで囲まれた非保護データ領域302が図2の非保護データ領域202に相当する。「SIGNATURE」というタグで囲まれた部分は保護領域をハッシュ化したデータを送信側装置の秘密鍵で暗号化した署名303であり、「CERTIFICATE」というタグで囲まれた公開鍵304には送信側装置から送られた公開鍵を納めている。署名303と公開鍵304が図2の検証情報領域203に相当する。「PROTECTED」タグ内に記述された「UNPROTECTEDTAG」は非保護データ領域である「UNPROTECTED」タグ内に記述されるタグを定義したタグリストであり、図2の非保護対象リスト204に相当する。

【0027】

保護データ領域301である「PROTECTED」タグ内には、改竄されてはいけない情報、例えば上述の書き換え操作コマンド3001やスケジュールデータ3002や、サーバに対して次のリクエストを返すためのURL3003が記述されている。

【0028】

一方、非保護データ領域302である「UNPROTECTED」タグ内には、一時的な情報である書き換えセッションID3004や更新日時情報3005が記述されている。

【0029】

以下図3とフローチャート図4とを交えながらクライアント側のアプリケーション部104にどのようにデータが渡されるか処理を説明する。

【0030】

受信部101からのテキストデータ30が渡されると、署名検証部102は「PROTECTED」タグで囲まれた保護データ領域301をハッシュ化する（S401）。次に署名303を公開鍵304で復号化する（S402）。保護データ領域301をハッシュ化したデータと署名303を復号化したデータとを比較する（S403）。比較結果が一致しなければ保護データ領域に誤りが発生しているのでデータは信用できないとし、破棄する（S404）。

【0031】

比較結果が一致した場合、保護データ領域301中の非保護対象リスト305と非保護データ領域302が署名検証部102から非保護データ検証部103へ送られる。

【0032】

非保護データ検証部103では非保護データ領域302で出現するタグが非保護対象リスト305に定義されているかチェックする（S405）。タグが未定義の場合は、そのタグは改竄されたタグか、もしくはアプリケーション部104にとって必要ないタグとして破棄する（S406）。

【0033】

アプリケーション部104には改竄のないことが保証された保護データ領域301のタグと、非保護対象リスト305に定義されていないタグを除いた非保護データ領域302のタグが渡される（S407）。上記スケジュールデータの例では非保護対象リスト305に書き換えセッションID3004のタグ「SESSIONID」や更新日時情報3005のタグ「MODIFIED」が定義されているので、非保護データ領域302に記述されている「SESSIONID」タグや「MODIFIED」タグはアプリケーション部104に渡してよい。また非保護データ領域302に記述されているコマンド3006のタグ「COMMAND」は非保護対象リスト305に定義されていないので改竄された可能性があり、信用できないタグとして破棄する。

【0034】

アプリケーション部104は非保護データ検証部103から受け取ったタグデータが保護データ領域または非保護データ領域のどちらに書かれていたかを意識する必要はない。なぜならタグ自身は署名検証部102および非保護データ検証部103によって正しいことが確認済みであり、非保護データ領域のタグのもつデータはもともと改竄については許容できるデータであるからである。もし改竄が許されないデータの場合は非保護対象リストからタグの定義を削除し、タグ自体を保護データ領域に記せばよい。

【0035】

以上の構成のように、非保護データ領域で使用するタグを保護データ領域内の非保護対象リストに定義することによって、データ全体に対してデジタル署名する場合に比べ署名確認に用いるデータの量を少なくして署名検証の効率を上げ、かつ非保護データ領域に記述したタグの信頼性を高く保ち、またアプリケーションにとってはタグの保護非保護状態を意識しないで処理することが可能となる。

【0036】

(実施の形態3)

図5は本発明の実施の形態3を示すシステムブロック図である。また必要に応じて図2を援用する。

【0037】

送信側データ処理装置51は送信データおよび非保護対象リスト204に加える情報種別を入力する入力部511と、非保護データ領域202で使用する情報の種別を非保護対象リスト204に定義する非保護対象リスト生成部512と、非保護対象リスト204に基づいて情報を保護データ領域201と非保護データ領域202に再配置するデータ配置部513と、保護データ領域201のデータについて改竄の有無を検出するための検証情報領域203を作成する署名生成部514と、データを外部に送信する送信部515とを備える。受信側データ処理装置10の構成は図1のデータ処理装置と同様の構成である。送信側データ処理装置51と受信側データ処理装置10は有線または無線のネットワークで接続されている。

【0038】

送信側データ処理装置51から受信側データ処理装置10へデータを送信する場合、送信側データ処理装置51では入力部511から非保護データ領域202で用いる情報種別を受け付ける。入力部511から入力された情報種別に基づいて非保護対象リスト生成部512で非保護対象リスト204を生成し保護データ領域201へ非保護対象リスト204を付加する。次にデータ配置部513は生成された非保護対象リスト204に基づき、送信データについて保護データ領域201に配置する情報種別と非保護データ領域202に配置する情報種別を判定し、保護データ領域201と非保護データ領域202内の情報の再配置を行う。具体的には非保護対象リスト204に定義された情報種別を非保護データ領域202に配置し、それ以外を保護データ領域201に配置する。次に署名生成部514は非保護対象リスト204を含む保護データ領域201のデータをハッシュ化した上、秘密鍵を用いて暗号化し署名を生成する。この署名と暗号化に用いた秘密鍵と対になる公開鍵を検証情報領域203として本文に付け加え、送信部515から受信側データ処理装置10へ送信を行う。受信側データ処理装置10の処理は実施の形態1と同様である。

【0039】

以上の構成のように、非保護データ領域で使用する情報種別を送信側で入力し、保護データ領域内に非保護対象リストとして生成付加し、保護データ領域と非保護データ領域に置くデータを判定することによって、受信側のアプリケーションその他の処理を一切変更することなく、特定の情報種別について保護状態を変更することが可能となる。したがってデータの運用に柔軟性を持たせることができる。

【0040】

またデータ全体に対してデジタル署名する場合に比べ署名確認に用いるデータの量を少なくして署名検証の効率を上げ、かつ非保護データ領域に記述したタグの信頼性を高く保ち、またアプリケーションにとってはタグの保護非保護状態を意識しないで処理することが可能となることは実施の形態1と同様である。

【0041】

(実施の形態4)

図6のテキストデータ60は公開鍵暗号によるデジタル署名を埋め込んだハイパーテキスト型言語XMLで記述されたスケジュールデータである。ここで図6で使用するタグの意味は図3と同様である。図6および必要に応じて図2と図5を援用しながら本発明の実施の形態4について詳細に説明する。

【0042】

ここで送信側データ処理装置51から送信するデータについて、図6の更新日時情報6005を非保護状態から保護状態に変更する必要がある場合を考える。

【0043】

図5の入力部511から非保護データ領域で使用するタグの集合を入力する。この時、更新日時情報6005は除く。すると非保護対象リスト生成部512は更新日時情報6005を除いた非保護対象リスト605を生成する。次にデータ配置部513は生成しなおされた非保護対象リスト605に基づいて非保護データ領域602にある更新日時情報6005を保護データ領域601に配置しなおす。その後、保護データ領域601について署名生成部514が署名603を計算し、公開鍵604と共に本文に検証情報領域として付加し、送信部515がデータを受信側データ処理装置10に送信する。

【0044】

受信側データ処理装置10では実施の形態2と同様の処理を行う。

【0045】

以上の構成のように、非保護データ領域で使用するタグを送信側で入力し、保護データ領域内に非保護対象リストとして生成付加し、保護データ領域と非保護データ領域に置くタグを判定することによって、受信側のアプリケーションその他の処理を一切変更することなく、特定のタグについて保護状態を変更することが可能となる。したがってタグの保護非保護状態を随時変更することができデータの運用に柔軟性を持たせることが可能となる。

【0046】

またデータ全体に対してデジタル署名する場合に比べ署名確認に用いるデータ

の量を少なくして署名検証の効率を上げ、かつ非保護データ領域に記述したタグの信頼性を高く保ち、またアプリケーションにとってはタグの保護非保護状態を意識しないで処理することが可能となることは実施の形態2と同様である。

【0047】

なお実施の形態1から実施の形態4において図2は、保護データ領域、非保護データ領域、検証情報領域の順に構成しているが、領域として区別が可能であれば任意の順序が可能である。また、保護データ領域内の非保護対象リストについても保護データ領域の他のデータと同様、デジタル署名の検証対象になっていれば任意の位置に置くことが可能である。

【0048】

なお実施の形態2と実施の形態4において、非保護対象リストに定義するタグをそれぞれ図3、図6のようにタグの内容名を並べて記述したが、非保護の対象になるタグが定義されていることが識別できれば、直接タグを記述したり、タグに代わる表現、例えばタグIDやタグの集合を表すメタ表現的な記述を使用してもよい。

【0049】

なお実施の形態3と実施の形態4において、入力部からは非保護対象リストに定義する情報種別もしくはタグを入力していたが、非保護データ領域と保護データ領域それぞれにどの情報種別もしくはタグを置くか識別できればよく、したがって保護データ領域で使用する情報種別もしくはタグを入力してもよい。また保護対象リスト生成部に記憶部を持ち前回の設定に対して変更部分についてのみ入力してもよい。

【0050】

【発明の効果】

本発明の請求項1におけるデータ処理装置では、非保護データ領域で使用する情報種別を保護データ領域内の非保護対象リストに定義することによって、データ全体に対してデジタル署名する場合に比べて署名確認に用いるデータの量を少なくして署名検証の効率を上げ、かつ非保護データ領域に記述した情報種別の信頼性を高く保ち、またアプリケーションにとっては各種別毎に保護非保護状態を

意識しないで処理することが可能なため、アプリケーションの処理が少なくなりサイズの縮小、処理速度の向上を計ることが可能となる。

【 0 0 5 1 】

本発明の請求項 2 におけるデータ処理装置では、非保護データ領域で使用するタグを保護データ領域内の非保護対象リストに定義することによって、データ全体に対してデジタル署名する場合に比べ署名確認に用いるデータの量を少なくして署名検証の効率を上げ、かつ非保護データ領域に記述したタグの信頼性を高く保ち、またアプリケーションにとってはタグの保護非保護状態を意識しないで処理することが可能なため、アプリケーションの処理が少なくなりサイズの縮小、処理速度の向上を計ることが可能となる。

【 0 0 5 2 】

本発明の請求項 3 におけるデータ処理装置では、非保護データ領域で使用する情報種別を送信側で入力し、保護データ領域内に非保護対象リストとして生成付加し、保護データ領域と非保護データ領域に置くデータを判定することによって、受信側のアプリケーションその他の処理を一切変更することなく、特定の情報種別について保護状態を変更することが可能となる。したがってデータの運用に柔軟性を持たせることができる。またデータ全体に対してデジタル署名する場合に比べ署名確認に用いるデータの量を少なくして署名検証の効率を上げ、かつ非保護データ領域に記述したタグの信頼性を高く保ち、またアプリケーションにとってはタグの保護非保護状態を意識しないで処理することが可能なため、アプリケーションの処理が少なくなりサイズの縮小、処理速度の向上を計ることが可能となる。

【 0 0 5 3 】

本発明の請求項 4 におけるデータ処理装置では、非保護データ領域で使用するタグを送信側で入力し、保護データ領域内に非保護対象リストとして生成付加し、保護データ領域と非保護データ領域に置くタグを判定することによって、受信側のアプリケーションその他の処理を一切変更することなく、特定のタグについて保護状態を変更することが可能となる。したがってタグの保護非保護状態を随時変更することができデータの運用に柔軟性を持たせることが可能となる。また

データ全体に対してデジタル署名する場合に比べ署名確認に用いるデータの量を少なくして署名検証の効率を上げ、かつ非保護データ領域に記述したタグの信頼性を高く保ち、またアプリケーションにとってはタグの保護非保護状態を意識しないで処理することが可能なため、アプリケーションの処理が少なくなりサイズの縮小、処理速度の向上を計ることが可能となる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態 1 のデータ処理装置を示すシステムブロック図

【図 2】

本発明の実施の形態 1 のデータ処理装置が扱うデータの構成図

【図 3】

本発明の実施の形態 2 のデータ処理装置が扱う XML データの構成図

【図 4】

本発明の実施の形態 2 のデータ処理装置の処理を示すフローチャート

【図 5】

本発明の実施の形態 3 のデータ処理装置を示すシステムブロック図

【図 6】

本発明の実施の形態 4 のデータ処理装置が扱う XML データの構成図

【符号の説明】

- 1 0, 5 1 データ処理装置
- 2 0 データ
- 3 0, 6 0 テキストデータ
- 1 0 1 受信部
- 1 0 2 署名検証部
- 1 0 3 非保護データ検証部
- 1 0 4 アプリケーション部
- 2 0 1, 3 0 1, 6 0 1 保護データ領域
- 2 0 2, 3 0 2, 6 0 2 非保護データ領域
- 2 0 3 検証情報領域

2 0 4, 3 0 5, 6 0 5 非保護対象リスト

3 0 3, 6 0 3 署名

3 0 4, 6 0 4 公開鍵

5 1 1 入力部

5 1 2 非保護対象リスト生成部

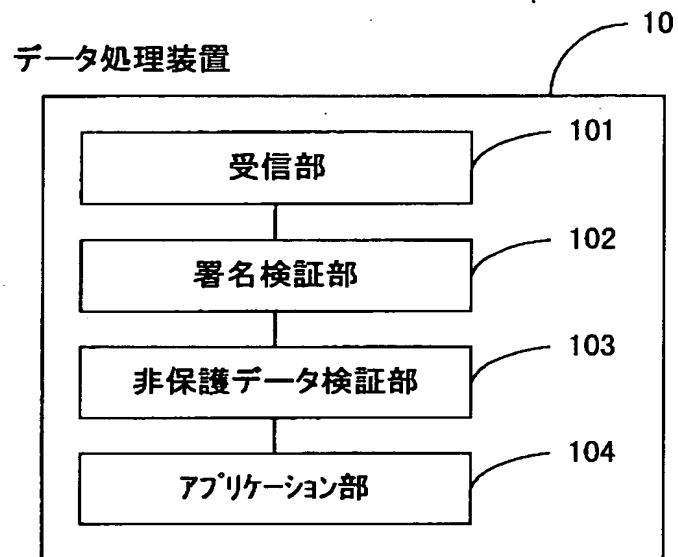
5 1 3 データ配置部

5 1 4 署名生成部

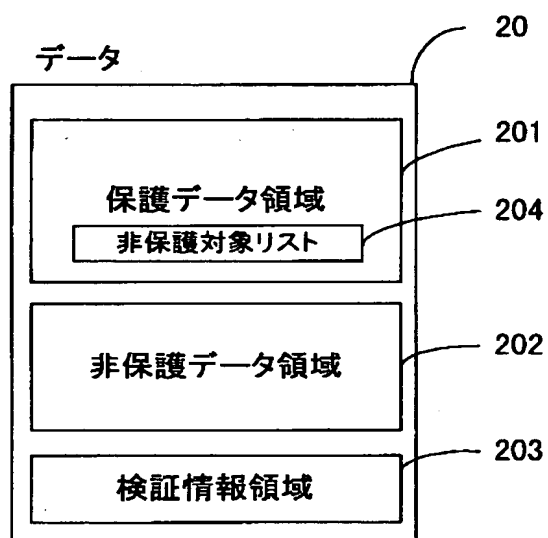
5 1 5 送信部

【書類名】 図面

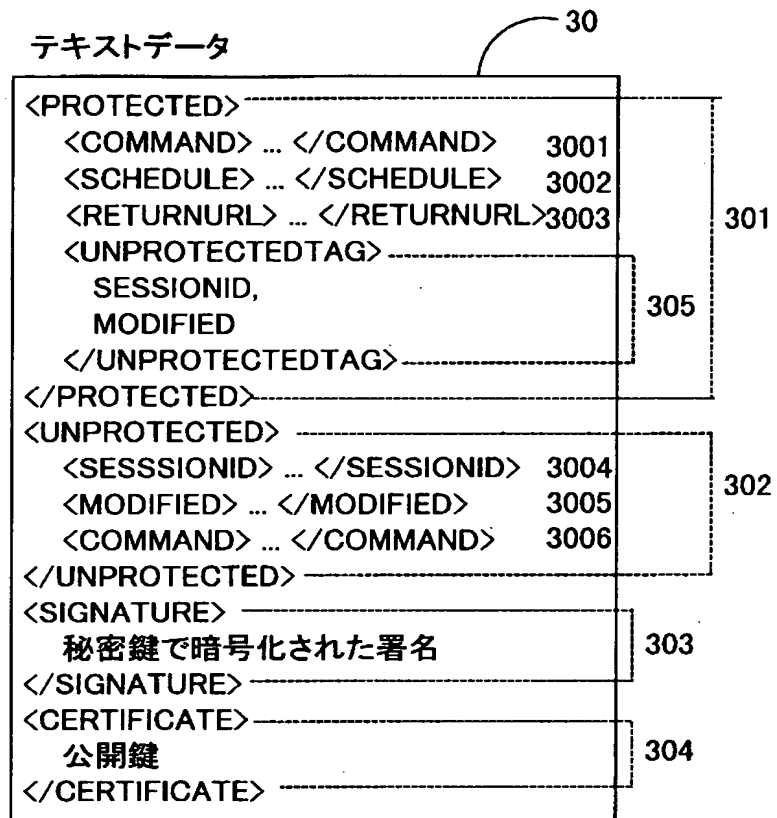
【図 1】



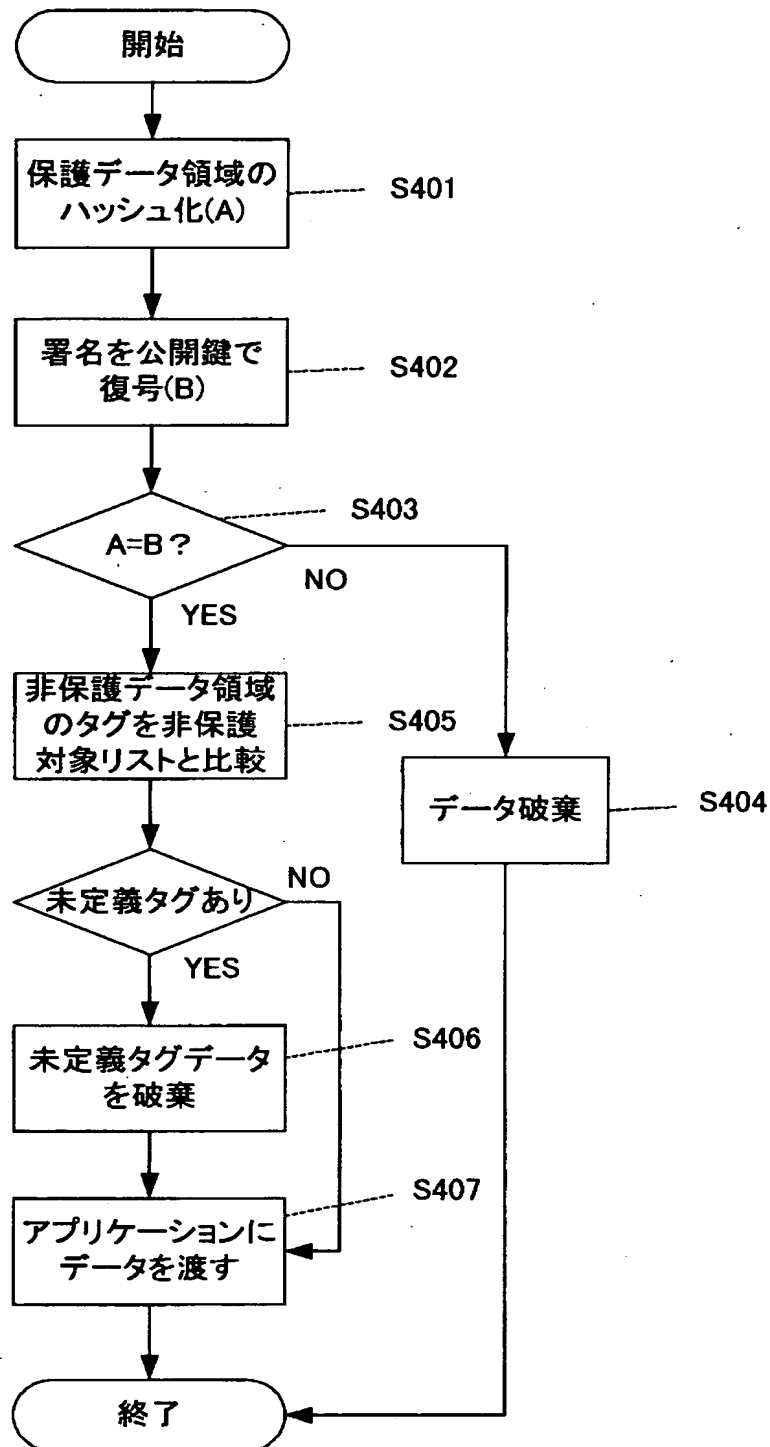
【図 2】



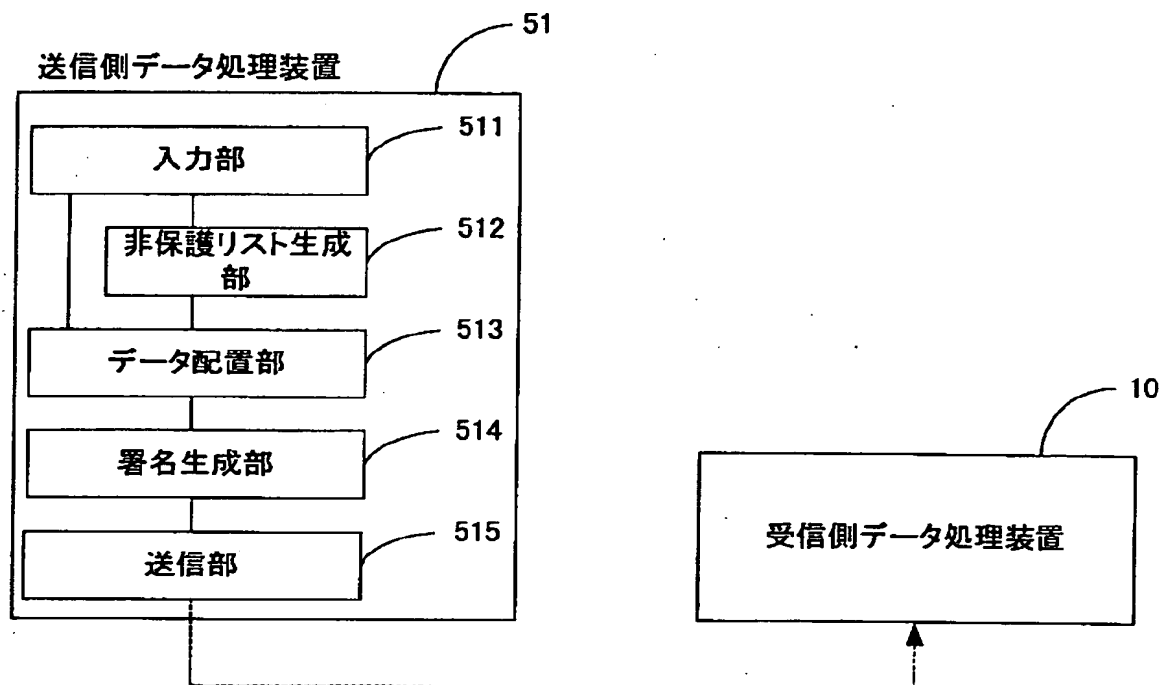
【図 3】



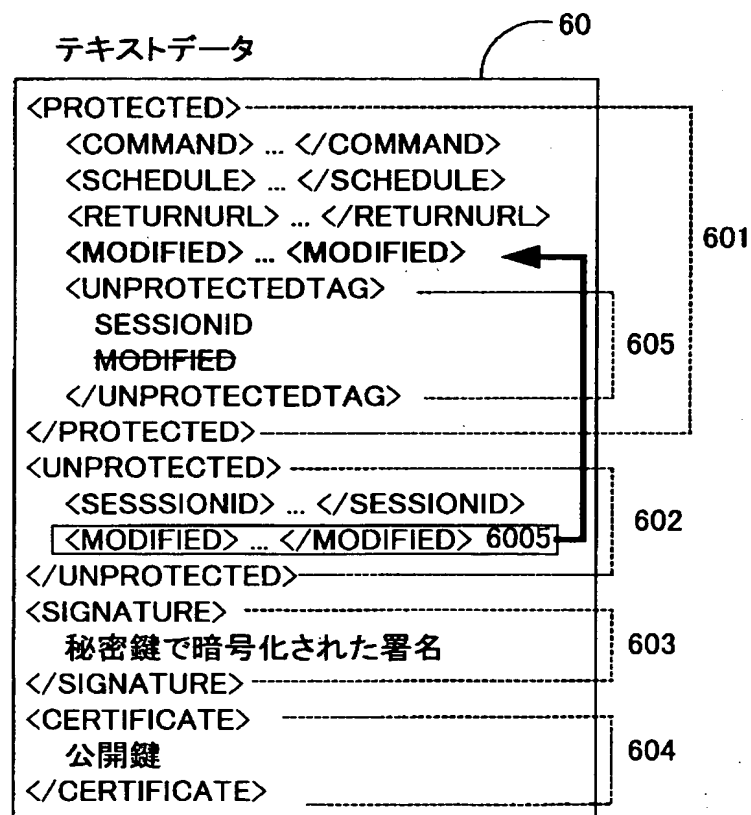
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 データにデジタル署名を付加しデータの正当性を検証する場合に、検証のコストを最小限に抑え、かつ非保護データについても信頼性を高め、データの保護非保護の設定が柔軟に変更できる技術を提供する。

【解決手段】 データを保護データ領域と非保護データ領域から構成し、デジタル署名は保護データ領域に対してのみ行う。非保護データ領域に納めるデータの種別を保護データ領域内に非保護対象リストとして保持し、非保護データ領域のデータと非保護対象リストとの比較で非保護データ領域内のデータの検証を行う。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社